OPENING REMARKS

COMMUNIST CHINESE CYBER ATTACKS, ESPIONAGE, AND THEFT OF AMERICAN TECHNOLOGY

The United States is under attack.

Cyber attacks and cyber espionage traced back to China have been dramatically increasing every year. What kind of damage is being done? How is our security being compromised? Shielding our digital infrastructure from attacks, and protecting intellectual property and classified information is strategically important to our national security. But how do we do that and what else needs to be done?

The Communist Chinese government has defined us as the enemy and is buying, building and stealing whatever it takes to contain and destroy us.

Chinese cyber attacks on U.S. assets now number in the thousands every year. The 2009 report on *China's Military Power* published by the Office of the Secretary of Defense (OSD) notes that, "numerous computer systems around the world, including those owned by the U.S. Government, continued to be the target of intrusions that appear to have originated within the PRC." One of the high value targets that Chinese cyber warriors have repeatedly attacked is the F-35 Joint Strike Fighter program which is the centerpiece of future American airpower capabilities.

The heavy use of outsourcing of computer and consumer electronic production to China, not only by American but also by Japanese, Taiwanese, German, and South Korean firms, has helped create a Chinese cyber threat that now compromises the security of the Western world.

Beijing has been given technology and a manufacturing base, making Western networks vulnerable to escalating Chinese capabilities.

The Office of the Secretary of Defense's 2010 annual report to Congress *Military and Security Developments Involving the People's Republic of China* outlined the challenge, "The PRC utilizes a large, well-organized network of enterprises, defense factories and affiliated research institutes and computer network operations to facilitate the collection of sensitive information and export-controlled technology."

The Chinese often use "patriotic hackers" as a cover for their activities, as well as corporate spies. But in that dictatorship the line between state and private efforts is blurred intentionally as to give Beijing plausible deniability.

Chinese thinking is based on slogans such as "Give Priority to Military Products" and "Combine the military with the civil." Thus, economic and commercial spying and theft are most frequently connected with tech-heavy industries deemed strategic by the regime. This includes computer software and hardware, biotechnology, aerospace, telecommunications, transportation and engine technology, automobiles, machine tools, energy, materials and coatings.

A new study by the Rand Corporation *Ready for Takeoff: China's Advancing Aerospace Industry* found, "China's aerospace industry has advanced at an impressive rate over the past decade, partly due to the increasing participation of its aerospace industry in the global commercial aerospace market and the supply chains of the world's leading aerospace firms…. China's growing civilian aerospace capabilities are unquestionably contributing to the development of its military aerospace capabilities"

Combine these commercial transfers with the espionage committed against American military programs like the F-35, and no one should be surprised by the roll out of the new J-20 "stealth" Chinese warplane last January. It was years ahead of what experts had predicted China could do on its own.

It is what happens during "peace time" that determines the balance of power that then governs the outcome when the peace breaks down. National security must be a constant concern.

Battleships and mass armies were left behind by aircraft and rockets. Now we must understand today's threats emanating from cyber space and technology transfers as well as from traditional practices of espionage.

Today, we have before us four experts on the connection of technology transfers and national power in a competitive world:

Mr. Pat Choate is currently the Director of the Manufacturing Policy Project, a private, non-profit, institute. Mr. Choate has written several widely acclaimed books, including *Agents of Influence* and *The High Flex Society* which document the decline in American competitiveness and the influence of foreign powers here in Washington DC.

Mr. Richard Fisher is a Senior Fellow with the International Assessment and Strategy Center. He is an active writer and scholar on China having worked for the Jamestown Foundation, the Center for Security Policy, and The Heritage Foundation. He is the author of *China's Military Modernization, Building for Regional and Global Reach,* and has been published in numerous newspapers and professional journals.

Mr. Edward Timperlake served as the Director of Technology Assessment, International Technology Security for the Department of Defense from 2003 to 2009. He indentified and

protected the Defense Department from espionage. He also served as the Defense Department representative to the National Counterintelligence Executive Committee. Before that he graduated from the Naval Academy and he served as a Marine fighter pilot. He co-authored the book, *Showdown, Why China Wants War with the United States.*

Mr. Adam Segal is a Senior Fellow with the Council on Foreign Relations and is an expert on security issues and Chinese policy. He has recently written a book titled, *Advantage: How American Innovation Can Overcome the Asian Challenge*. He has taught at Vassar College and Columbia University and holds a Ph. D. from Cornell University.